NATIONAL INSTITUTE OF TECHNOLGY PATNA

Department of Computer Science and Engineering

END SEMESTER EXAMINATION, DEC 2020

Program: B. Tech. in Computer Science and Engineering

Course Title: Information Security (Code: CS6404), Credit: 3

Duration: 02:00 Hours | Date: 22 May 2021 | Full Mark: 40

Instructions:

1. *Keep your copy CLEAN. HIGHLIGHT/ UNDERLINE the KEY parts.*
2. Write your NAME and ROLL NO. on the top of every page.
3. *Answer all the Questions.*
4. *Candidates have to answer all parts of a particular Question at one place only.*
5. *The figures in the Right hand margin indicate full marks and this question paper has two pages.*

---

1. Consider the last three digits of your Roll Number (in $1806\#\#\#$ format) as secret message. *(For example if your roll number is* 1806055 *then your secret message is* 55*).* You are transmitting the secret message using RSA. For configuring the RSA algorithm it's given $p = 19$ and $q = 13$ and $e = 11$. Determine your private key. Compute the cipher text. Showing calculation of each steps are must. There are many numbers in the range of 1 to 200 for which calculation of cipher will not be possible. In such case you must mention the reasons with justification. [10]
2. Enumerate all the properties of cryptographic hash function. List down the cryptographic uses of hash functions. Describe the SHA1 with a neat diagram of one SHA1 operation. [3+2+5]
3. What is access control and what is authentication. What are the different ways of authenticating users? What are different types of information security policy? What do you understand by guideline, base line and procedure in information security? [3+2+2+3]
4. The block cipher given in Algorithm 1 takes 8 bit plain text blocks (b) and 4 bit key (k) to encrypt plain text (m). The algorithm divides the input message m in 8 bit blocks (b_i) where $i = 1, 2, \ldots, (|m|/8)$. (converts m into binary stream).

   Your plain text (secret message) is last three digits of your roll number in 8 bit binary concatenated at the end of 10111010. (If your roll number is 1806001 in decimal then

Algorithm 1 Simple Cipher

procedure ENCRYPTION
    Input: message m, Key k
    Initialize C=NULL
    $N \leftarrow (|m|/8)$
    $m \rightarrow b_1, b_2, \ldots b_N$
    for each block b_i **do**
        for each $j = 1$ to 2 **do**
            $b_i \rightarrow L_j$ and R_j
            $R_j \leftarrow R_j \oplus k$
            $R_j \leftarrow R_j'$ (complement operation)
            $R_j \leftarrow R_j \oplus L_j$
            if j==2 **then**
                $c_i = L_j R_j$
                continue
            end if
            $L_{j+1} \leftarrow R_j$ and $R_{j+1} \leftarrow L_j$
            $k \leftarrow k << 2$ (circular Left shift by 2)
            $c_i \leftarrow L_{j+1} R_{j+1}$
        end for
        Cipher $C \leftarrow C + c_i$ (where $+$ represent concatenation operation)
    end for
end procedure

the last three digits are 001 which will be converted in binary as 00000001 and your plain text will be 1011101000000001).

Calculate the cipher text in 8 bit integer using secret key $k = 1111$. Show the calculation in detail without hiding any step. [10]

END